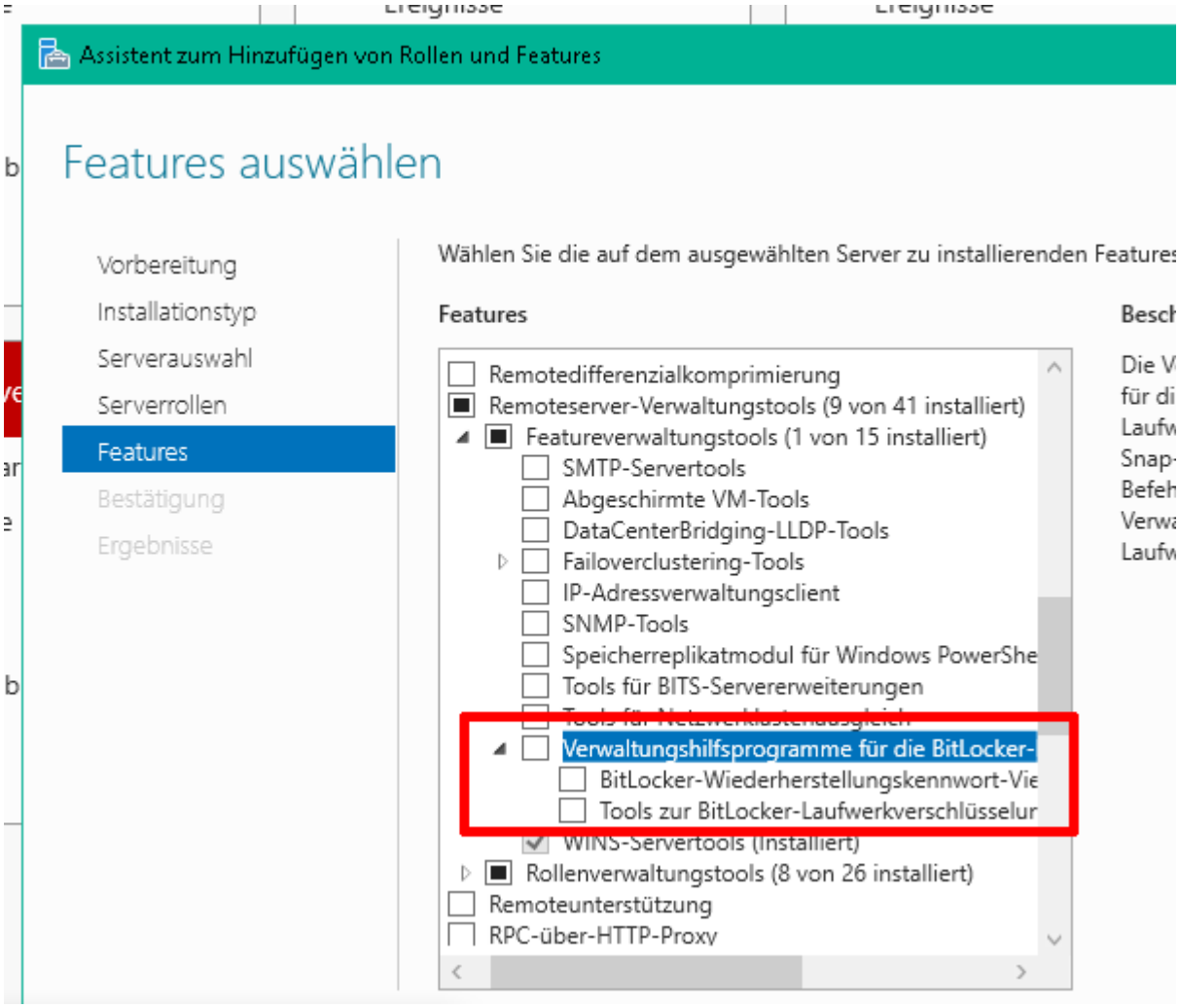
Bitlocker in einer AD-Umgebung

Diese Anleitung umfasst:

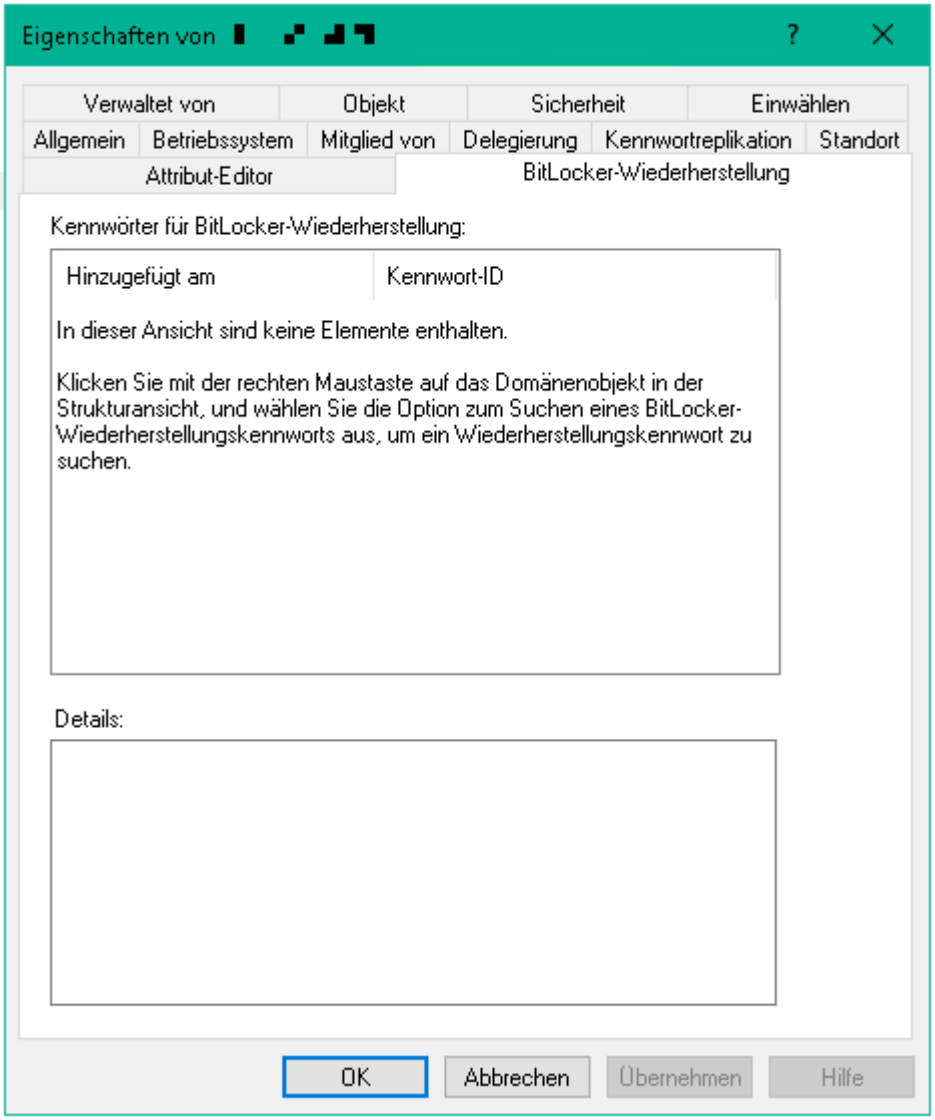
- Schlüssel in der AD gespeichert
- TPM wird vorausgesetzt
- Bitlocker wird am Rechner manuell aktiviert

Feature auf dem DC

Damit der im AD abgelegte Schlüssel in der Konsole „Active Directory Users & Computers“ nachgeschlagen werden kann, muss über den Servermanager folgendes Feature installiert werden. Dies muss auf jedem Domain Controller geschehen, über den die Schlüssel verwaltet werden sollen.



In der Konsole sollte das hinterher so aussehen:



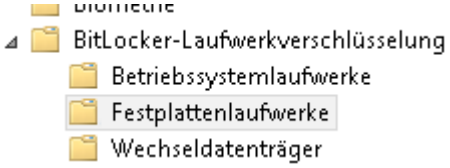
Das Feature installiert nicht nur die Tools, sondern auch die Schemaerweiterung im AD, in der die Informationen abgelegt werden. Mittels folgenden Powershell-Befehl.

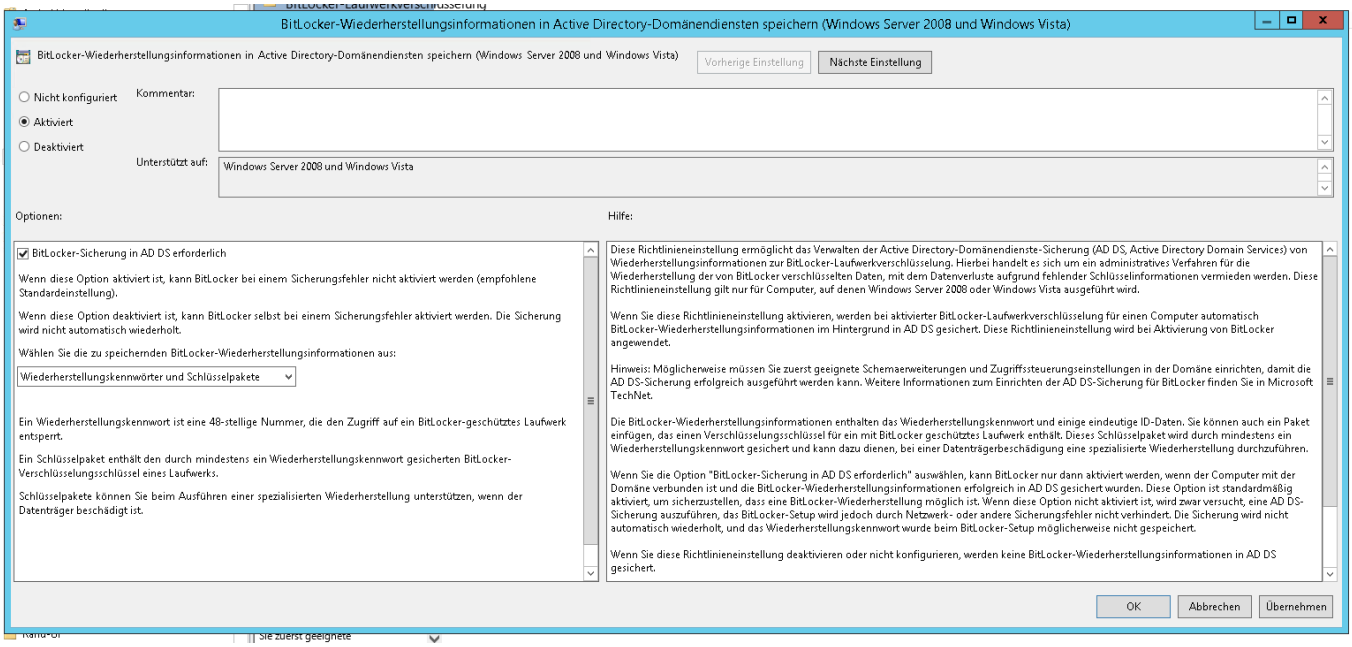
```
Get-ADObject -SearchBase ((GET-ADRootDSE).SchemaNamingContext) -Filter {Name
-like 'ms-FVE-*'}

DistinguishedName             Name                          ObjectClass
ObjectGUID
-----------------             ----                          -----------
----------
CN=ms-FVE-KeyPackage,CN=Sc... ms-FVE-KeyPackage             attributeSchema
80dd0b7b-4c78-4305-9844-ce...
CN=ms-FVE-RecoveryGuid,CN=... ms-FVE-RecoveryGuid           attributeSchema
d9b3a270-ce1a-4514-9f73-c2...
CN=ms-FVE-RecoveryInformat... ms-FVE-RecoveryInformation    classSchema
82dac378-fa82-46ae-a49f-16...
CN=ms-FVE-RecoveryPassword... ms-FVE-RecoveryPassword       attributeSchema
1b97cf96-65b7-4939-834c-ff...
CN=ms-FVE-VolumeGuid,CN=Sc... ms-FVE-VolumeGuid             attributeSchema
47080651-54da-4a8b-bfc9-a0...
```

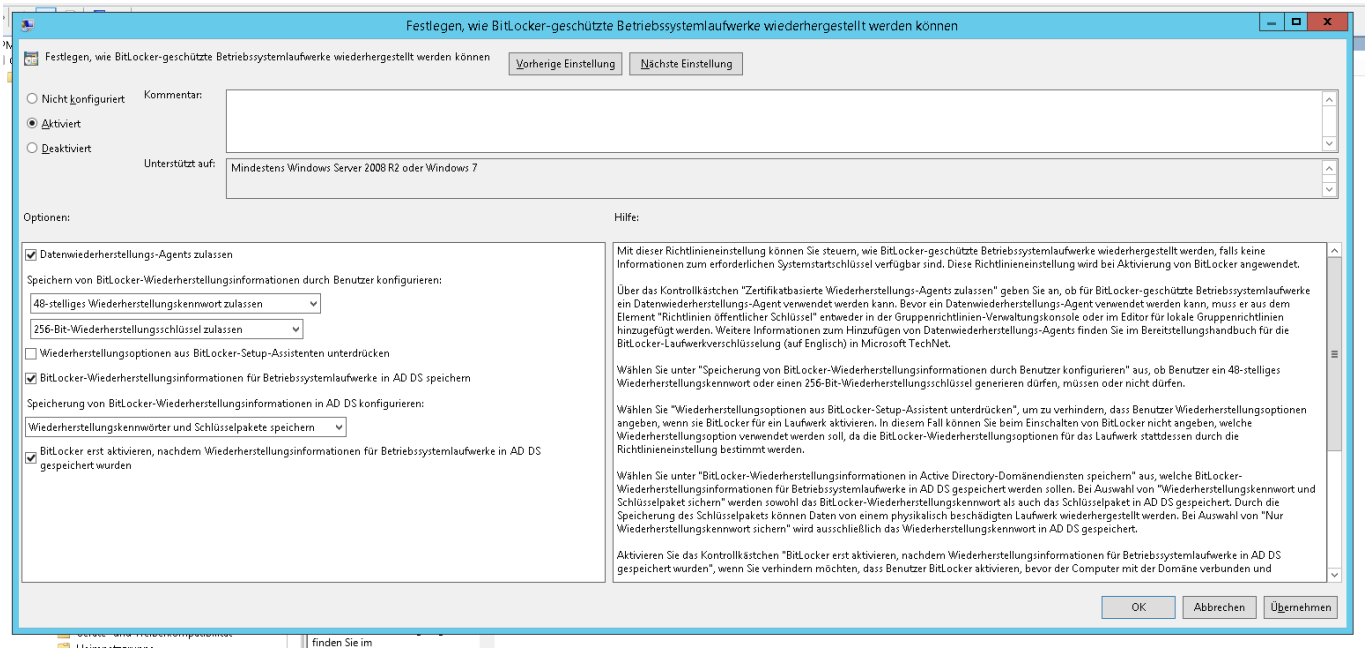
Gruppenrichtlinie für die Clients

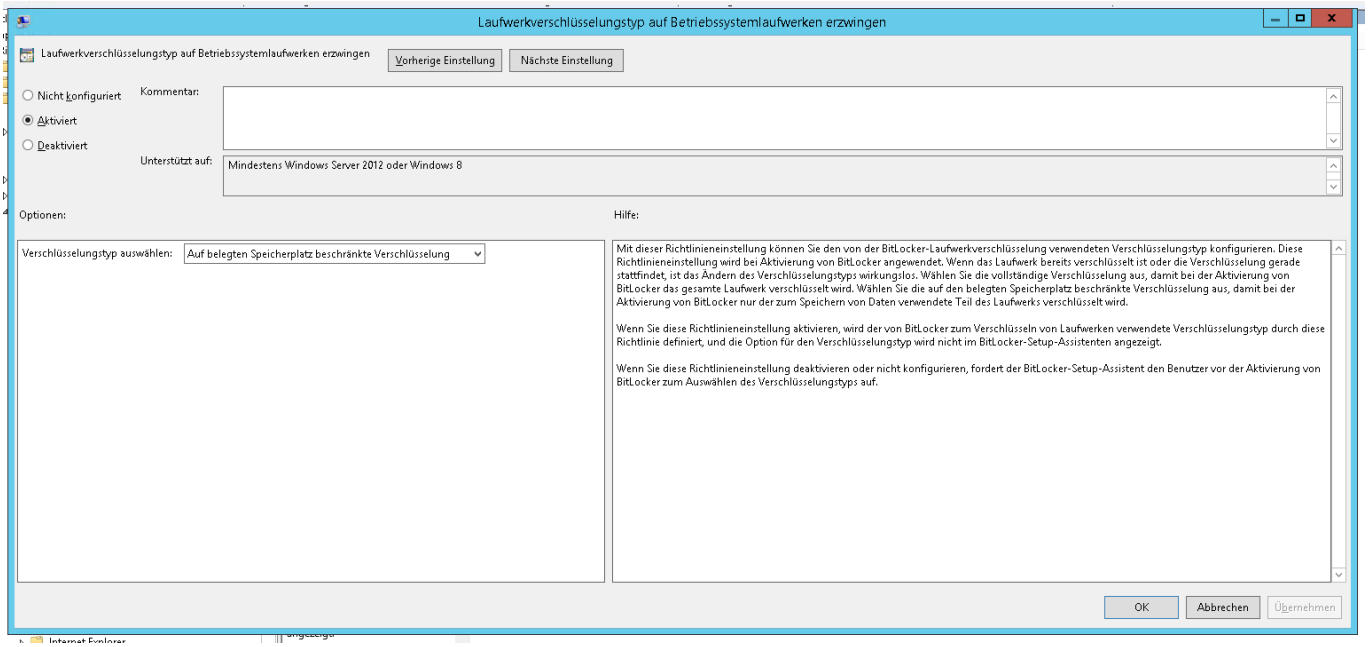
`Computerkonfiguration → Richtlinien → Administrative Vorlagen → Windows-Komponenten → Bitlocker-Laufwerksverschlüsselung`

Die Konfiguration muss jeweils für das Betriebssystem-Laufwerk, (weitere) Festplattenlaufwerke sowie Wechseldatenträger erfolgen:









TPM ja oder nein?

Per Powershell

```
PS> Get-Tpm

TpmReady                  : False
TpmPresent                : True
ManagedAuthLevel          : Full
OwnerAuth                 :
OwnerClearDisabled        : True
AutoProvisioning          : Enabled
LockedOut                 : False
SelfTest                  : {191, 191, 245, 191...}
```

Per WMI

```
wmic /namespace:\\root\cimv2\security\microsofttpm path win32_tpm get /value
```